НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210720.4 | 20 июля 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО Advantech R-SeeNet

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	R-SeeNet: 2.4.12
Дата выявления	16 июля 2021 г.
Дата обновления	16 июля 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-21805	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально созданного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных в скрипте ping.php. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС) Рекомендации по устранению: обновить программное обеспечение	9.8

MITRE: CVE-2021-21804	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код PHP в целевой системе посредством отправки специально созданного запроса. Уязвимость обусловлена некорректной проверкой входных данных при включении PHP-файлов в параметр «sub_opt» скрипта options.php. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H CWE-98: Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP) Рекомендации по устранению: обновить программное обеспечение	8.1

Ссылки на источники	https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1274 https://www.cybersecurity-help.cz/vdb/SB2021071609 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1273